The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

I also certify that the attached copy of the request for grant of a Patent (Form 1/77) bears an amendment, effected by this office, following a request by the applicant and agreed to by the Comptroller-General.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

-registration under the Companies Act does not constitute a new legal entity but merely jects the company to certain additional company law rules.

CERTIFIED COPY OF PRIORITY DOCUMENT

Signed

Dated 12 TH MARCH 2002

0028935.5

Patents Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

1/77

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP9 1RH

1. Your reference
CTV/P45208

2. Patent application number
(The Patent Office will fill in this part)
0028935.5

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Swivel Technologies Limited
Bleach Garth
Little Beck
Whitby
North Yorkshire
YO22 5EZ

Patents ADP number *(if you know it)*
07975394001

If the applicant is a corporate body, give the country/state of its incorporation
UK

4. Title of the invention
Secure file transfer method and system

5. Name of your agent *(if you have one)*
Harrison Goddard Foote

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Tower House
Merrion Way
Leeds
LS2 8PA

Patents ADP number *(if you know it)*
14571001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*
	11/7) 5/9/01	NO 13/9/01
~~GB~~	~~0021964.2~~	~~07/09/2000~~

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application

Date of filing
(day / month / year)

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form

Description 10

Claim*(s)* -

Abstract -

Drawing*(s)* 10 +10

10. If you are also filing any of the following, state how many against each item.

Priority documents

Translations of priority documents

Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*

Request for preliminary examination and search *(Patents Form 9/77)*

Request for substantive examination *(Patents Form 10/77)*

Any other documents *(please specify)*

11. I/We request the grant of a patent on the basis of this application.

Signature

Date 27/11/2000

12. Name and daytime telephone number of person to contact in the United Kingdom

Chris Vaughan 0113 290 1400

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

SECURE FILE TRANSFER METHOD AND SYSTEM

The present invention relates to a method and system for confirming that an electronic data file downloaded from a remote computer server by way of the Internet, the World-Wide Web (the Web) or otherwise has been obtained from an authentic or authorised source.

With the recent and rapid expansion of the Internet and the Web and other protocols for transferring large amounts of data between remote computers by way of telecommunications links and the like, it has now become increasingly easy to copy and transfer files containing video and audio recordings as well as many other software applications. Standard file formats such as MP3, MPEG, JPEG and many more allow high quality digital audio and video recordings to be downloaded for very little, if any, cost and to be played back at any convenient time, possibly by way of portable units such as pocket MP3 players. While these developments are readily welcomed by consumers, it is very difficult to enforce copyright in audio and video recordings when these can be downloaded so easily, and this can result in a significant loss of revenue to the companies that make and release these recordings, as well as to the authors and performers of the recorded works. Traditionally, audio and video recordings have been sold to the public in the form of data carriers such as compact discs and the like, the distribution of which was heretofore relatively easy to control. This is no longer the case, and there is consequently a need to provide some form of control over the distribution of authentic recordings.

The problem is compounded by the fact that many data files which can be downloaded by a consumer at no cost from potentially inauthentic sources may contain viruses or Trojan horses which can infect and disrupt the consumer's computer or network. This can have devastating and expensive consequences, and is a high price to pay just to obtain free data files.

It is apparent that there is a need to provide a method and system for the secure transfer of data files from authentic sources, whereby a data file provider can provide an assurance to consumers that the data files thus provided are free of viruses and Trojan horses. Furthermore, there is a need to provide some way of raising revenue for the data file provider and the authors and performers of the works provided by the data file provider.

According to a first aspect of the present invention, there is provided a method of transferring a data file from a first computer having a first telecommunications address to a second computer having a second telecommunications address, comprising the steps of:

i) transmitting a request for the data file from the second computer to the first computer, the request including data identifying the data file and the second telecommunications address;

ii) in the first computer, wrapping or encrypting the data file within an executable file adapted to unwrap or decrypt the data file only upon activation by a unique key code;

iii) assigning a unique identification string to the executable file in the first computer, the unique identification string being further associated in the first computer with the second telecommunications address;

iv) transmitting the executable file and the unique identification string from the first computer to the second computer;

v) causing a message to be displayed by the second computer showing the unique identification string and requesting a user to call a predetermined telephone number from a telephone operated by the user;

vi) receiving a telephone call from the telephone operated by the user, determining its telephone number and receiving the unique identification string from the user;

vii) in the first computer, generating a pseudorandom string, associating the pseudorandom string with the unique identification string and the telephone number of the telephone operated by the user, and transmitting the pseudorandom string to the telephone operated by the user;

viii) applying a mask code, known to the user and to the first computer, to the pseudorandom identification string so as to generate a volatile identification code in accordance with predetermined rules;

ix) transmitting the volatile identification code to the first computer, either from the telephone operated by the user in which case the volatile identification code is transmitted together with the telephone number of the telephone operated by the user, or from the second computer in which case the volatile identification code is transmitted together with the second telecommunications address, the telephone number or the second telecommunications address respectively serving to identify the second computer, the user and the executable file;

x) in the first computer, checking that the volatile identification code matches a volatile identification code generated therein by applying the mask code to the pseudorandom string and, if so;

xi) transmitting the key code to the second computer so as to enable the executable file to unwrap or decrypt the data file and to install this on the second computer.

For the avoidance of doubt, the expressions "first computer" and "second computer" are not to be understood as being limited to first and second stand-alone computer devices, but are intended to encompass first and/or second computer networks, such as local or wide area networks and the like, as well as portable computers such as personal digital assistants and third (or subsequent) generation mobile telephones or communicators

In this first preferred embodiment, the first computer generally has stored therein a library of different data files, each of which may have a permanent identification code different from the unique identification string, which is individually generated for each executable file upon respective generation thereof. The permanent identification codes are provided so as to allow a user of the second computer to browse through the library of data files and to select data files for transmission. The library of data files may be remotely browsable from the second computer by way of a website or the like hosted by or otherwise linked to the first computer.

When the user has made his selection, for example by way of the website, selection information together with information identifying the second computer, for example an Internet Protocol (IP) address, is transmitted to the first computer. The first computer then wraps or encrypts the selected data file in the executable file in a manner which is known to those of ordinary skill in the art and assigns a unique identification string to the executable file. The unique identification string may include characters which identify the data file in a way which is meaningful to a human being. For example, where the data file is an MP3 audio file of a particular piece of music, the identification string may include characters which spell out a title of the piece of music. The unique identification string, in addition to identifying the executable file, also enables the first computer to identify the second computer and/or the user and/or the telephone operated by the user by correlating this data with the unique identification string in the first computer.

Instead of the first computer having stored therein the library of data files, the library of data files may be stored on and browsed by way of a third computer separate from the first and second computers. When a user makes a selection from the library, the third computer is then arranged to generate the unique identification string and to transmit this, together with the data file and the information identifying the second computer, such as an IP address, to the first computer by way of a telecommunications link. The data file is then wrapped or encrypted in the executable file at the first computer as discussed above.

The executable file and the unique identification string are then transmitted from the first computer to the second computer by way of a modem or Internet link. When they arrive at the second computer, a message may be displayed so as to alert a user that the executable file and the unique identification string have arrived. In a preferred embodiment, the message prompts the user to make a telephone call to a predetermined telephone number, either by way of a landline telephone or, more preferably, by way of a mobile telephone. When the user calls the predetermined telephone number, the telephone number of the telephone operated by the user is automatically determined by known means and the user is then asked to give the unique identification string so as to enable the executable file to be correlated in the first computer with the telephone number of the telephone operated by the user.

In a particularly preferred embodiment, when the user calls the predetermined telephone number with details of the unique identification string, a charge is made to the user's telephone account in respect of the data file requested from the first computer. This charge can be collected by the provider of the data file by way of a prearranged contract with a telephone service provider to which the user subscribes. Charging protocols of this type are already known in relation to vending machines which may be operated by way of a mobile telephone, whereby a user makes a selection from the vending machine, calls a predetermined telephone number with details of his or her selection, and the vending machine is then activated to dispense the selection to the user while a charge is made to the user's telephone account so as to pay for the selection.

The first computer then generates a pseudorandom string, correlates this with the unique identification string (and thereby with the executable file and data identifying the user, e.g. the telephone number of the telephone operated by the user or the IP address of the second computer), and then transmits the pseudorandom string to the telephone operated by the user, for example by way of a short messaging service (SMS) message.

The user then applies the mask code, which in a preferred embodiment comprises the last four digits of the telephone number of the telephone operated by the user but which may comprise any predetermined combination of digits from the telephone number or another prearranged numerical string, to the pseudorandom string so as to generate a volatile identification code in accordance with predetermined rules, further details of which are provided below. The volatile identification code is then transmitted by the user to the first computer, either by way of, for example, an SMS message from the telephone operated by the user or by way of the second computer and an Internet or modem link. When transmitting the volatile identification code by either of these routes, further data identifying the user and hence the particular data file transaction is also transmitted so as to enable the first computer to identify the transaction to which the volatile identification code relates. These further data may comprise the telephone number of the telephone operated by the user or the IP address of the second computer, both of which are correlated in the first computer with the unique identification string and hence the particular transaction.

When the first computer receives the volatile identification code and the associated data identifying the transaction, it performs a check to see that the volatile identification code matches a volatile identification code generated independently in the first computer by applying the mask code to the pseudorandom string. If the volatile identification codes are found to match, safe receipt of the executable file is thereby confirmed to the first computer.

The first computer then transmits the key code to the second computer, generally by way of and Internet or modem link. Upon receipt of the key code at the second computer, the executable file is enabled so as to unwrap or decrypt the data file and to install this on the second computer for use by the user. The key code is preferably a unique code generated within the executable file when it is first compiled and distributed, but not transmitted therewith.

When the data file is installed on the second computer, the executable file may be adapted to install the data file only in a specific memory location within the second computer. For example, the executable file may ask the operating system of the second computer (e.g. DOS) for a free memory location (e.g. a diskvolume name) and any other necessary system parameter and will then install the data file to this memory location, generally in read-only format.

In a particularly preferred embodiment, the installation process at the second computer generates an electronic certificate which authenticates the origin of the data file and also registers the data file to the user. The electronic certificate may include details of, say, the IP address of the second computer, details identifying the data file and the memory location where it is stored in the second computer. The electronic certificate is displayed when the data file is first installed, and may also be displayed each subsequent time that the data file is opened by the user. It is preferred that the data file is stored at the memory location in a protected read-only format, and that it can only be opened from that memory location with simultaneous at least temporary display of the electronic certificate. In this way, the data file is protected from infection by viruses which may enter or be present in the second computer, since the data file is locked and owned by itself within the memory of the second computer.

The electronic certificate may also contain further details, such as a system time and date in real time when activated, various copyright identifiers and registered trade marks relating to the provider of the data file and/or the executable file, identification details of the second computer (such as its IP address) and identification details of the data file. Some or all of these details may be merged into a short animation watermark image (which may nominally be animated at a speed of 16 frames per second and shown for several seconds), and a sound file relating to the title of the data file may also be generated and activated upon opening the data file. The watermark image is difficult to recreate by counterfeit measures, and thereby helps to guarantee that the data file is from an authorised source, free from viruses and licensed to an authorised user. It is intended that the charge raised for use of the data file is low enough so as to make forgery of the electronic certificate not worthwhile.

Referring now to the mask code, this may take various forms. In a currently preferred embodiment, a person is issued with or selects a four digit numerical string, for example 3928, analogous to the well-known PIN codes currently used when operating automated teller machines (ATMs). However, different lengths of mask code may be used as appropriate. In a particularly preferred embodiment, the mask code is based on the digits of the telephone number of the telephone from which the user calls the predetermined telephone number with details of the identification string and the volatile identification code. For example, the mask code may be set as the last four digits of the user's telephone number, say 3928.

In order to generate the volatile identification code, the user or the first or second computer takes the first digit of the mask code, in this example 3, and notes the character in third position (say from left, to right) along the identification string. The user or computer then takes the second digit of the mask code, in this example 9, and notes the character in ninth position along the identification string, and so on for the digits 2 and 8 of the mask code. The characters selected from the identification string form the volatile identification code which is used for secure identification purposes. The prime security feature is that the mask code is never transmitted between the computers and/or the telephone, and is thus safe from interception by unauthorised third parties.

It will be apparent that in the embodiment described hereinabove, the identification string must be at least ten characters long, since a mask code made up of the numbers 0 to 9 requires at least ten positions along the identification string to be functional. However, a person of ordinary skill will appreciate that different mask codes and string lengths may be used as required by selecting appropriate coding schemas. It is to be emphasised that the identification string assigned to the executable file by the first computer in response to a request for the data file will be different for each request, and that it will therefore be extremely difficult to determine a given mask code given a series of potentially interceptable identification strings and volatile identification codes.

For a better understanding of the present invention and to show how it may be carried into effect, reference shall now be made, by way of example, to the accompanying drawings in which:

FIGURE 1 is a flow diagram depicting one arrangement of the present invention;

FIGURE 2 shows a user operating the second computer;

FIGURE 3 shows a display on the second computer offering a data file for transfer thereto;

FIGURE 4 shows a display on the second computer prompting the user to call in with the unique identification string;

FIGURE 5 shows the user calling in with the unique identification string;

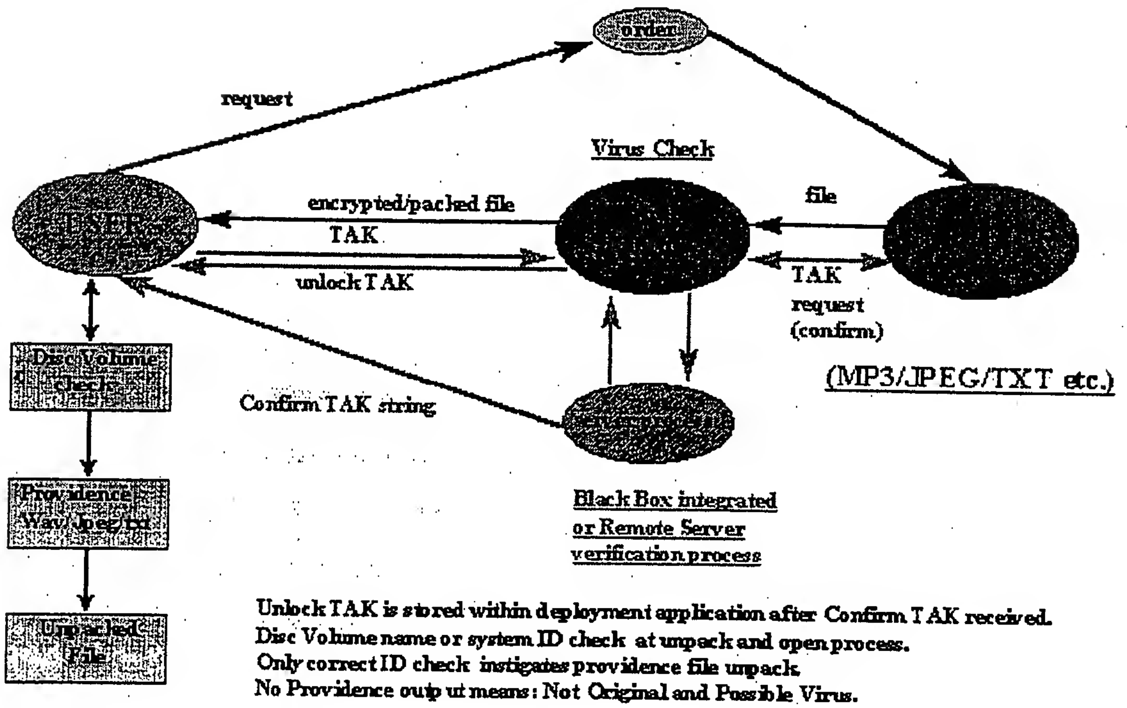
FIGURES 6 and 7 show the pseudorandom string being transmitted to the user's telephone and illustrate the application of the mask code thereto so as to generate the volatile identification code;

FIGURE 8 shows a display on the second computer prompting the user to input the volatile identification code;

FIGURE 9 shows a display on the second computer as the executable file is being operated so as to unwrap or install the data file; and

FIGURE 10 shows an electronic certificate displayed on the second computer when the data file has been unwrapped or installed.

TAK Application - PROVIDENCER



Unlock TAK is stored within deployment application after Confirm TAK received.
Disc Volume name or system ID check at unpack and open process.
Only correct ID check instigates providence file unpack.
No Providence outp ut means: Not Original and Possible Virus.

Fig. 1

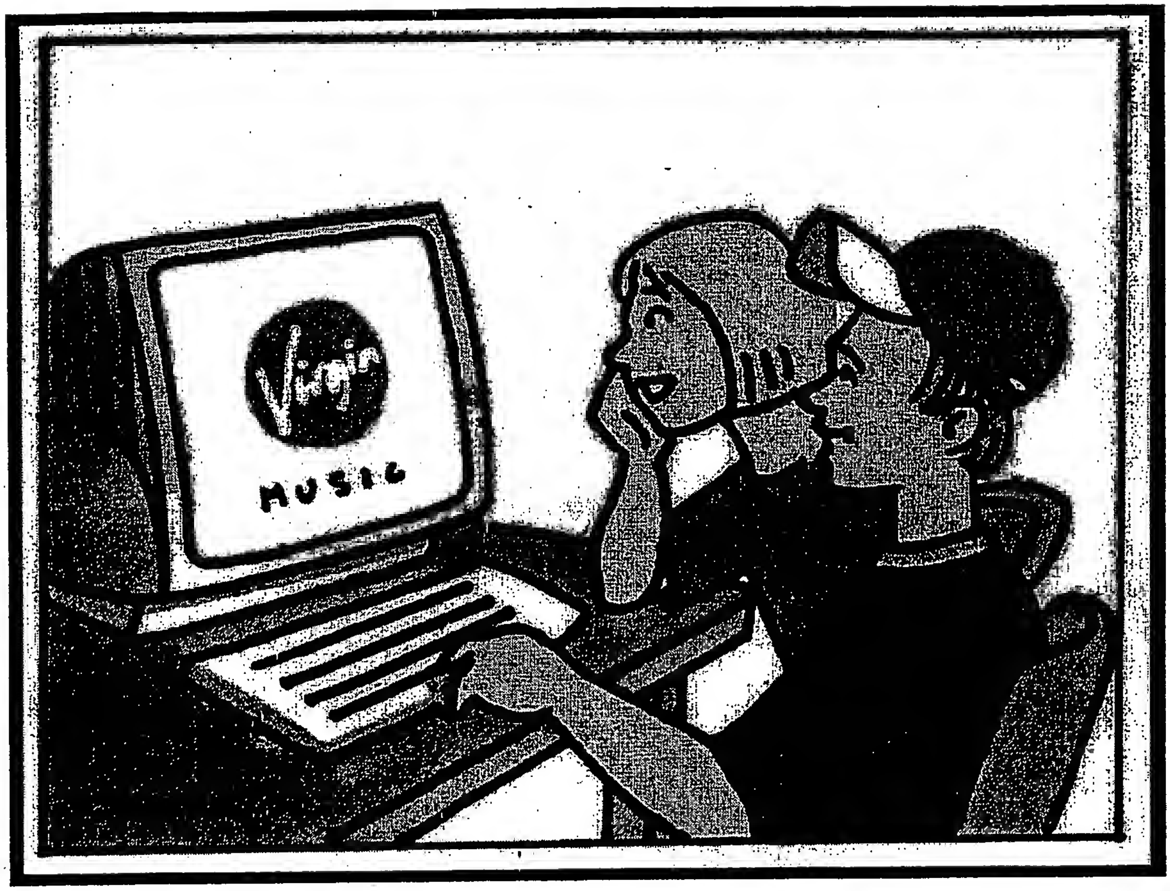


Fig. 2

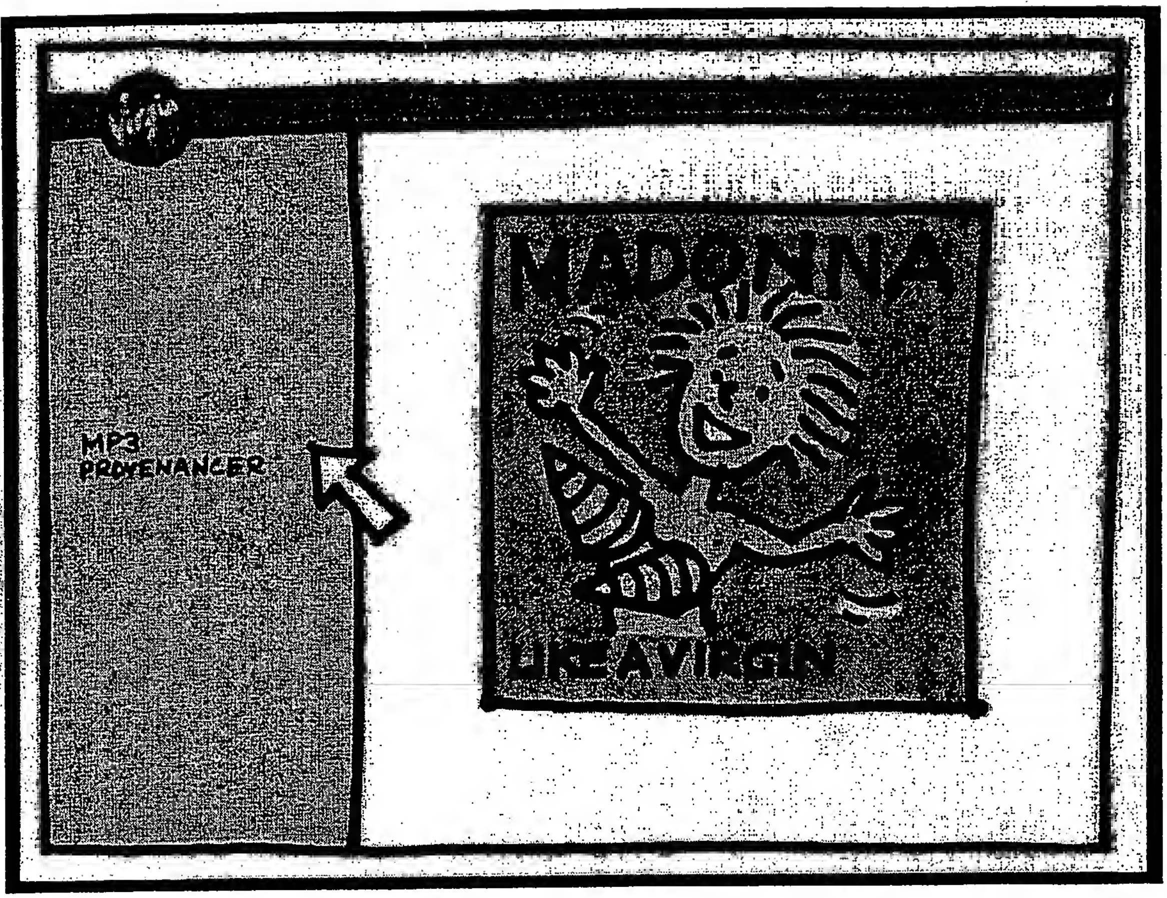
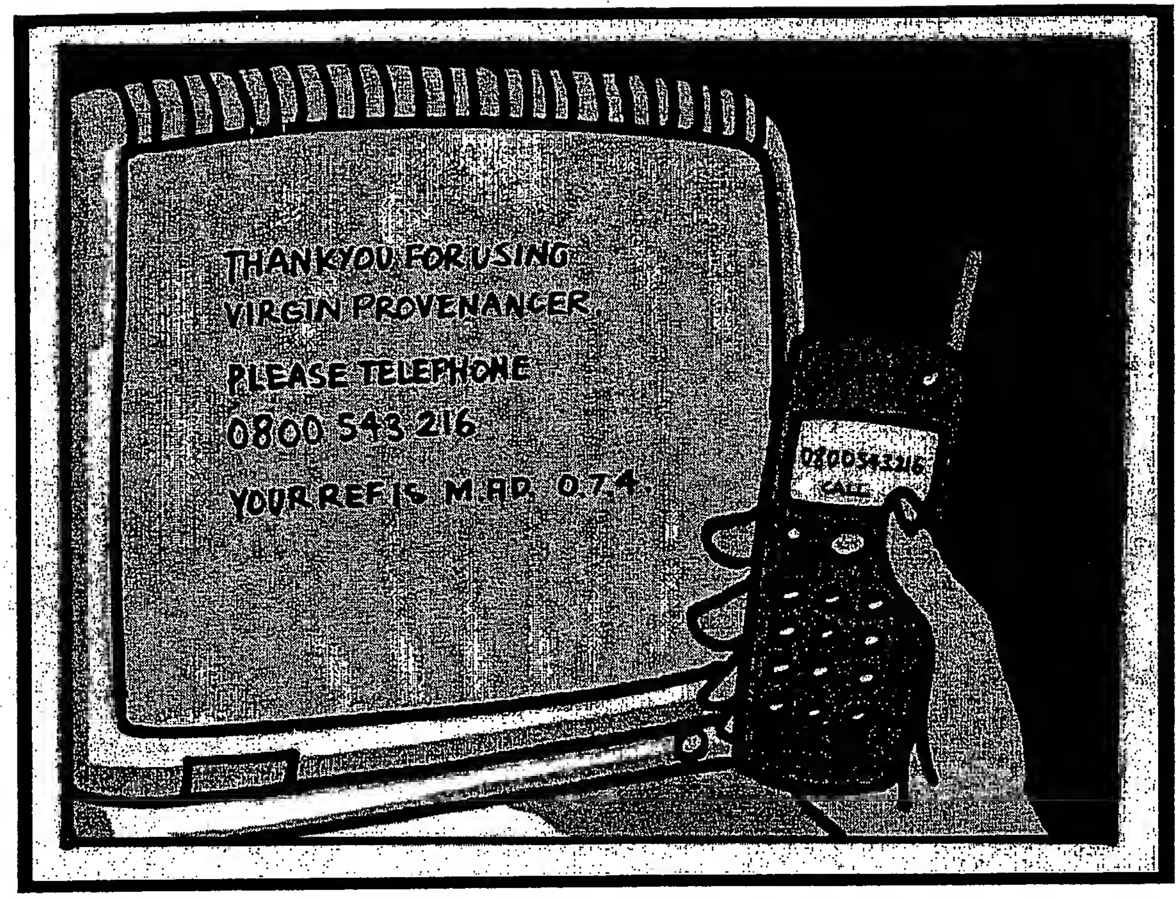


Fig. 3



THANKYOU FOR USING
VIRGIN PROVENANCER.

PLEASE TELEPHONE
0800 543 216

YOUR REF IS M.AD. 074.

Fig. 4

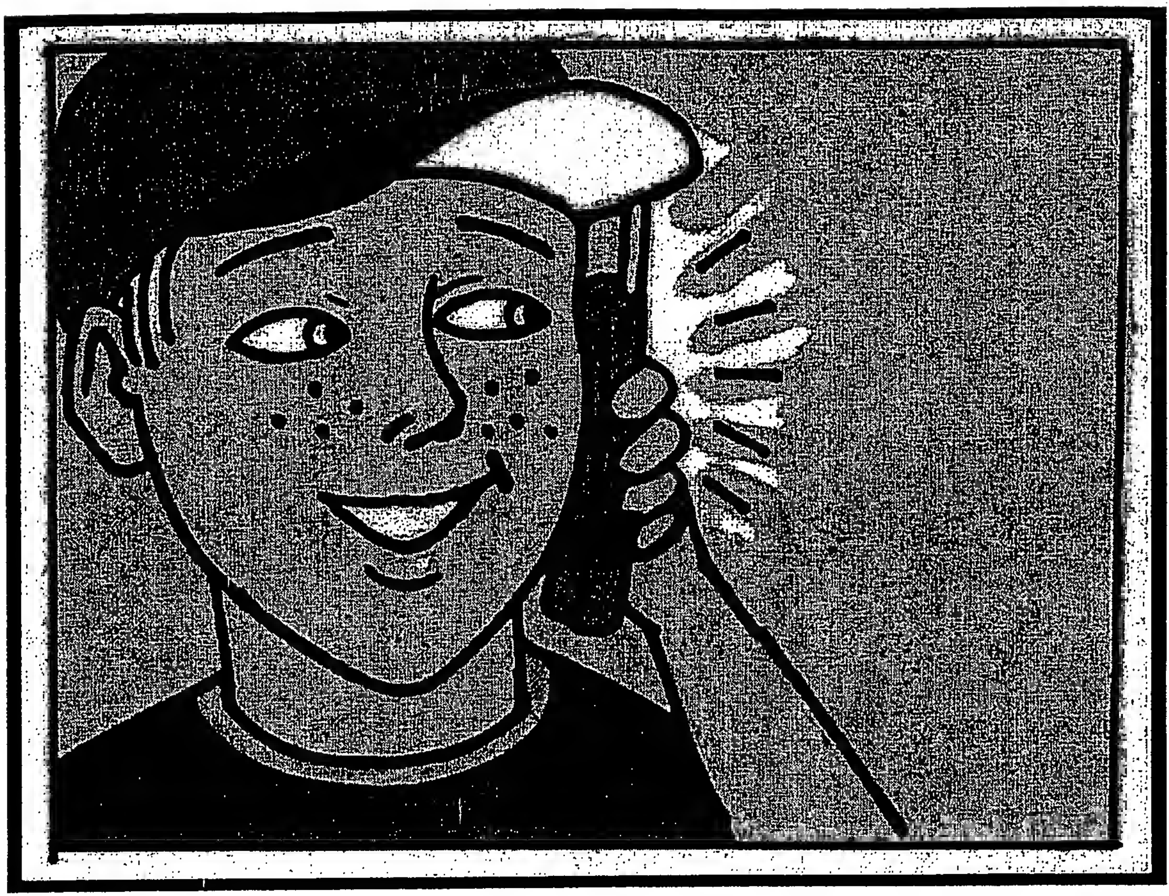


Fig. 5

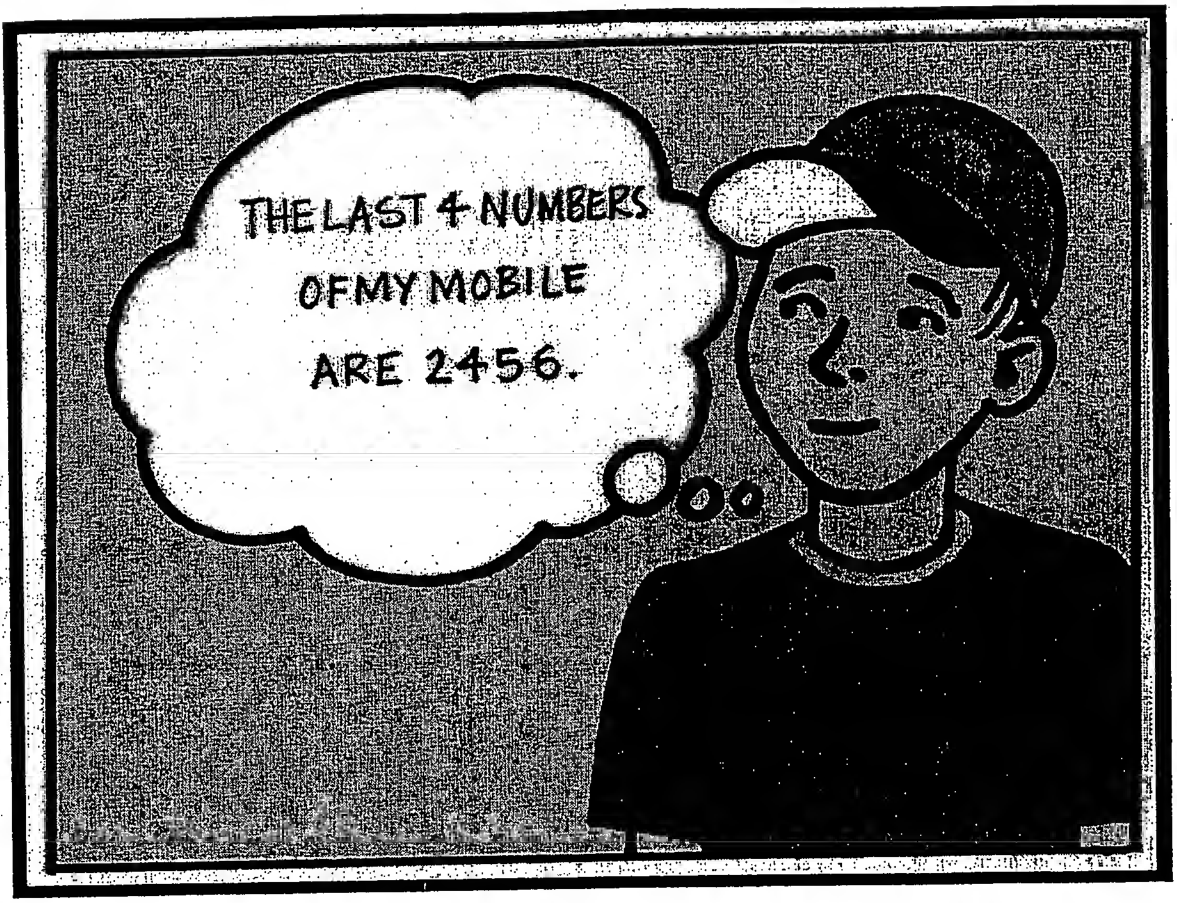


Fig. 6

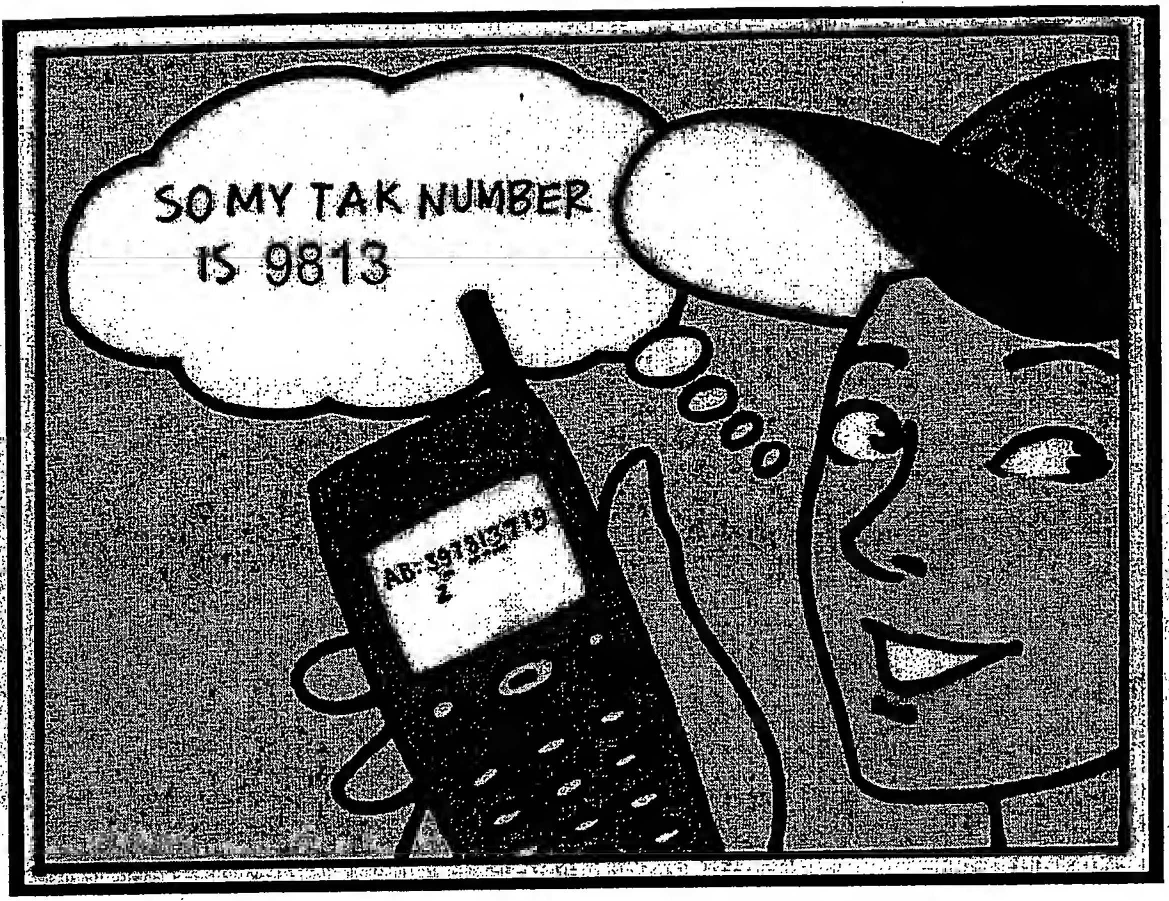


Fig. 7

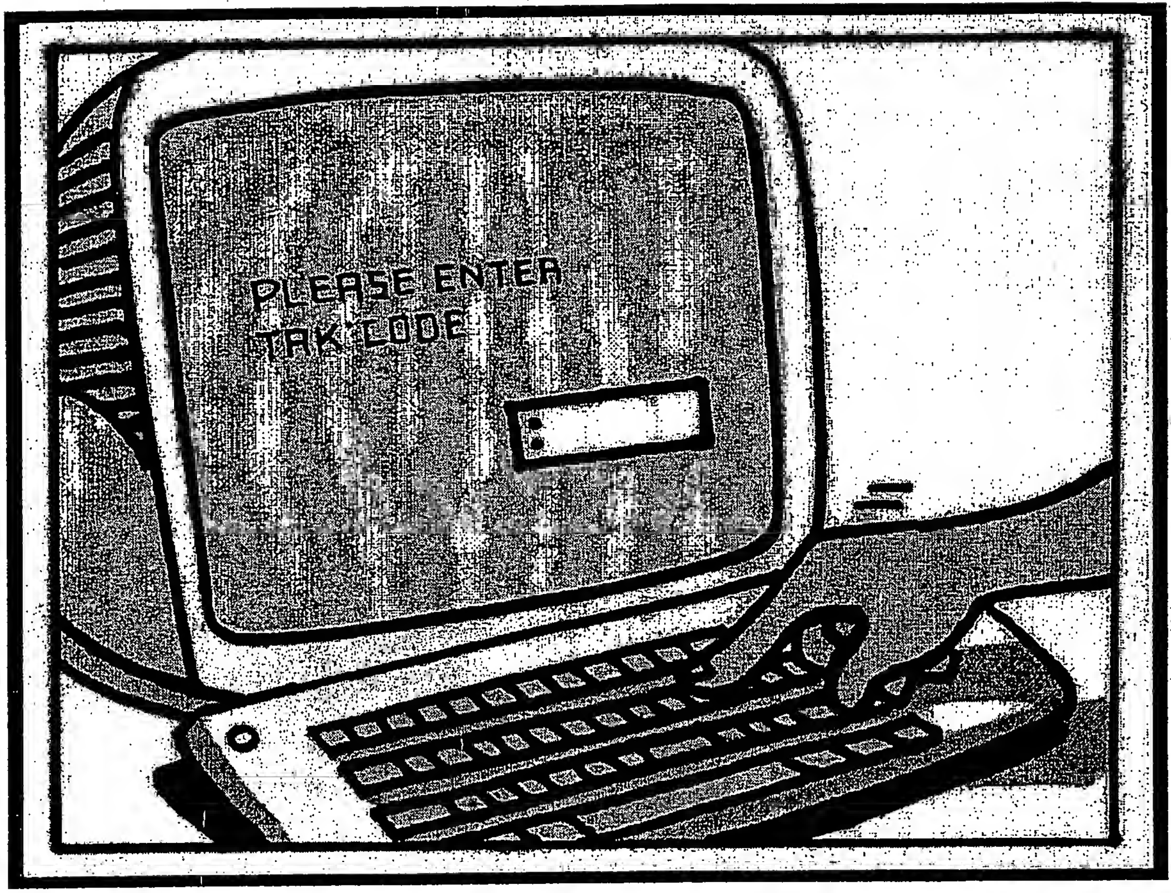
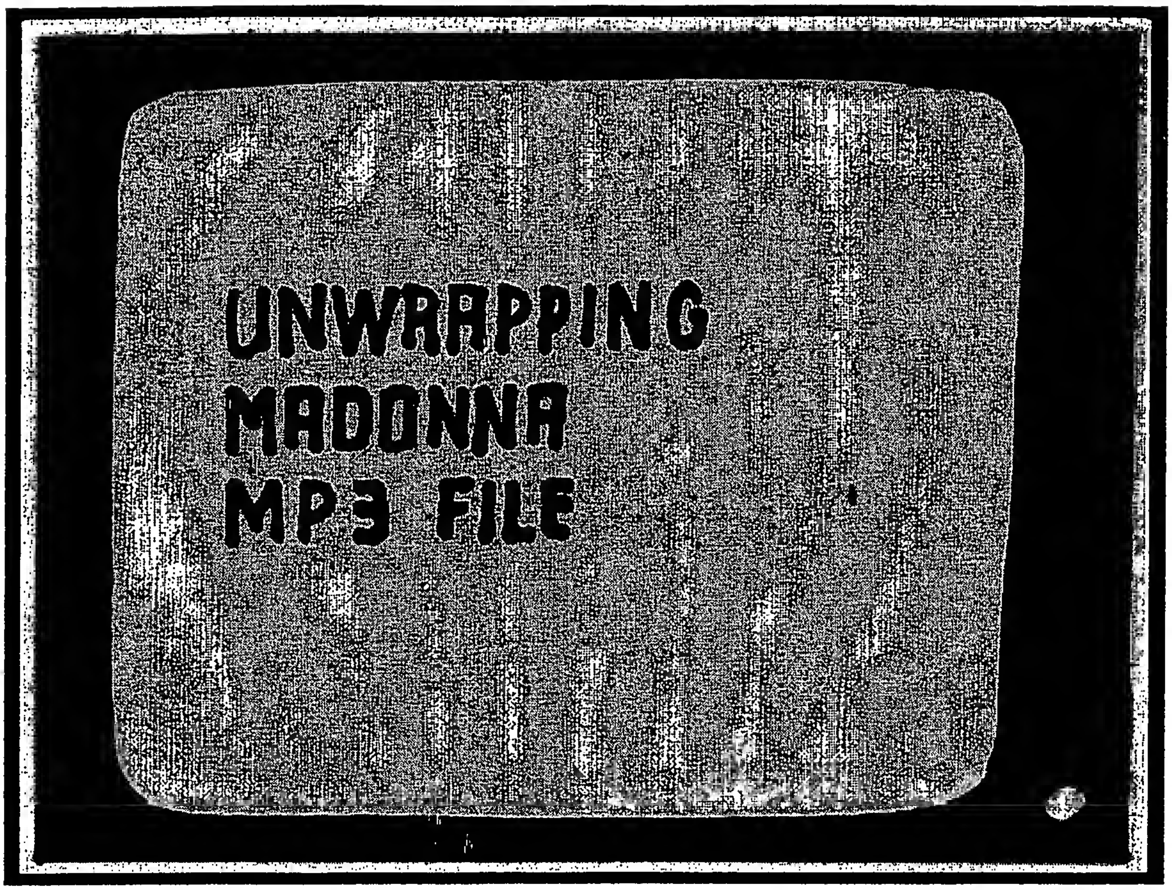


Fig. 8



UNWRAPPING
MADONNA
MP3 FILE

Fig. 9

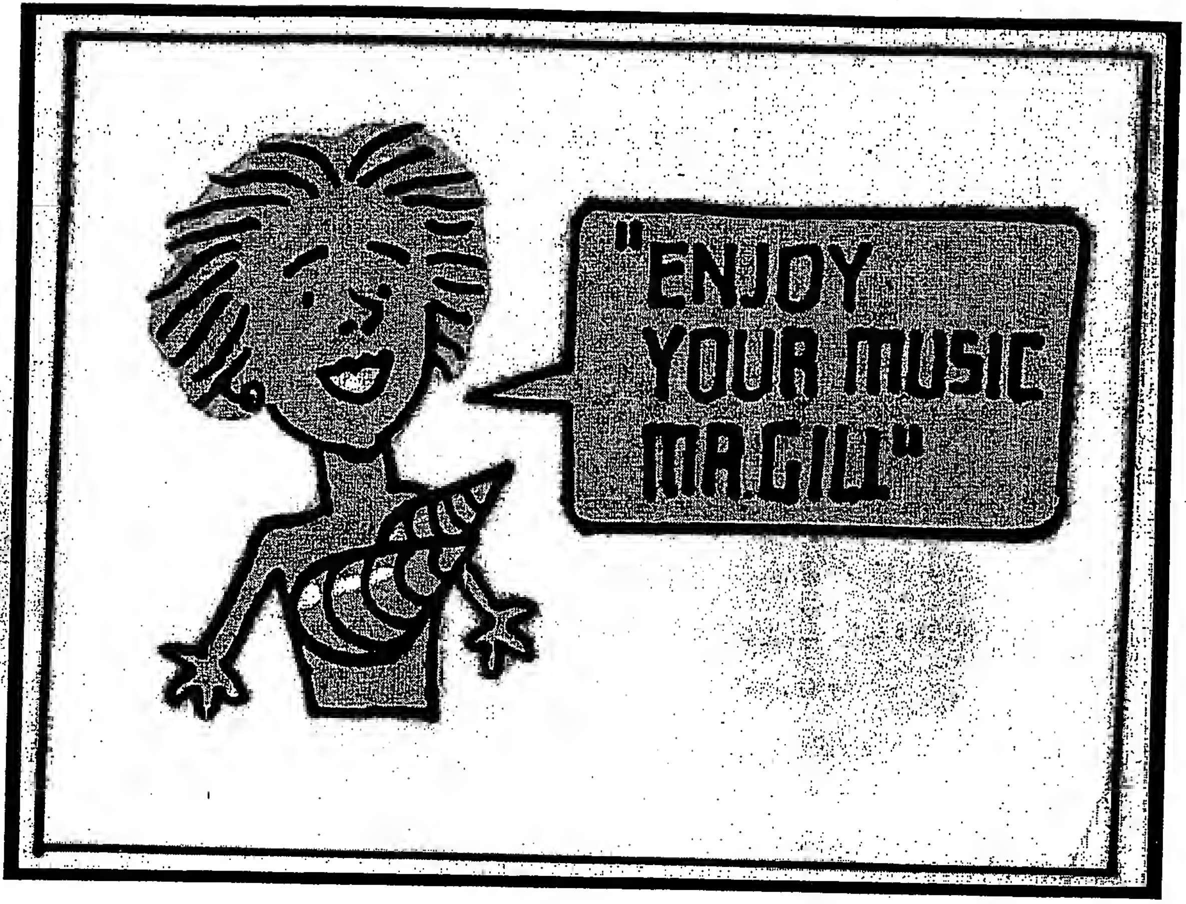


Fig. 10